UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/765,907	01/19/2001	Stephen M. Trimberger	X-714 US	9367

24309	7590	08/07/2006	

XILINX, INC
ATTN: LEGAL DEPARTMENT
2100 LOGIC DR
SAN JOSE, CA 95124

EXAMINER
COLIN, CARL G

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
	09/765,907	TRIMBERGER, STEPHEN M.
Office Action Summary	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *18 May 2006*.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-4,7,12,13,15 and 21* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-4,7,12,13,15 and 21* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 5/18/2006 has been entered.

Response to Arguments

2.   In response to communications filed on 5/18/2006, applicant amends claims 1 and 12.

The following claims 1-4, 7, 12-13, 15, and 21 are presented for examination.

2.1   Applicant's remarks, page 5, filed on 5/18/2006, with respect to the rejection of claims 1

and 12 have been fully considered, but they are not persuasive. Applicant's arguments do not

comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which

he or she thinks the claims present in view of the state of the art disclosed by the references cited

or the objections made. Further, they do not show how the amendments avoid such references or

objections. The claims have been amended to recite truncating m least significant bits from a

first binary number that represents the first number of oscillations and m least significant bits

from a second binary number that represents the second number of oscillations wherein m is

greater than 0; generating a ratio between the first binary number and the second binary

number... however, the claims as amended are not fully supported in the specification and the

rejection of claims 1-4, 7, 12-13, 15, and 21 is set forth below.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner

and process of making and using it, in such full, clear, concise, and exact terms as to enable any

person skilled in the art to which it pertains, or with which it is most nearly connected, to make

and use the same and shall set forth the best mode contemplated by the inventor of carrying out

his invention.

Claims 1 and 12 and the intervening claims are rejected under 35 U.S.C. 112, first

paragraph, as failing to comply with the written description requirement. The claim contains

subject matter, which was not described in the specification in such a way as to reasonably

convey to one skilled in the relevant art that the inventor(s), at the time the application was filed,

had possession of the claimed invention. Applicant's disclosure fails to recite "truncating m

least significant bits from a first binary number that represents the first number of oscillations

and m least significant bits from a second binary number that represents the second number of

oscillations wherein m is greater than 0; generating a ratio between the first binary number and

the second binary number...." The only section in the specification disclosing, truncating least

significant bit, is found on page 13, paragraph 32, with reference to figure 5. The specification

on the other hand, mentions shortening the fingerprint by ignoring the least significant bits

diminishes security. In addition, the ratio is generated from dividing the count value of the

oscillators and the binary equivalent of the ratio is used as a fingerprint (as described on

paragraph 31 of the specification). There is no description of the claimed limitations as amended

in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the

time the application was filed, had possession of the claimed invention.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or

described as set forth in section 102 of this title, if the differences between the subject matter

sought to be patented and the prior art are such that the subject matter as a whole would have

been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which

the invention was made.

Claims 1-4, 7, 12-13, 15, and 21 are rejected under 35 U.S.C. 103(a) as being

unpatentable over US Patent 5,970,142 to **Erickson** in view of US Patent 6,260,146 to **Mos et**

al.

As per claim 1, **Erickson** discloses a method of securing communication of configuration

data between a field programmable gate array (FPGA) and an external storage device

comprising: a plurality of configurable logic elements within the FPGA being programmable

with configuration data to implement a desired circuit design, for example (see column 3, lines

5-21); transmitting encrypted configuration data from the storage device to the FPGA, for

example (see column 3, lines 34-36); and a decryption circuit coupled to received encrypted

configuration data, the decryption circuit configured to decrypt the encrypted configuration data

in the FPGA using the fingerprint as a decryption key to extract the configuration data, for

example (see column 3, lines 34-42). **Erickson** discloses a security circuit comprising a key

generator for generating a key (column 2, lines 30-31) and the security circuit also comprises a

security initialization circuit for generating initialization data to be used for

encryption/decryption (column 4, lines 44-65) that meets the recitation of fingerprint element for

generating fingerprint representing inherent manufacturing process variations unique to the

FPGA. **Erickson** does not explicitly disclose generating the key from a ratio of the number of

oscillator counts. **Mos et al** in an analogous art teaches counting a first number of oscillations of

a first oscillator and a second number of oscillations of a second oscillator during a

predetermined time interval and generating a ratio between the first and the second binary

numbers of oscillations (see column 14, lines 27-41 and 50-55) wherein the ratio is a fingerprint

that represents an inherent manufacturing process characteristic unique to the FPGA (see column

7, lines 1-9 and column 10, lines 44-48). **Mos et al** discloses using binary data that represent the

number of oscillations (as shown in figure 5 and column 9, lines 37-45), but does not explicitly

disclose to ignore the least significant bit. It would have been obvious to one of ordinary skill in

the art at the time the invention was made to ignore the least significant bit as a design choice in

order to adjust to the desired values. Therefore, it would have been obvious to one of ordinary

skill in the art at the time the invention was made to modify the method of key generation of

Erickson to apply the concept of random number generator of **Mos et al** of measuring

propagation delays and combining the propagation delays to generate the fingerprint because this

technique provides a way of generating true random binary numbers with high statistical quality

(see column 6, line 63 through column 7, line 9). The motivation to do so is given by **Mos et al**

who teaches, a secure signature is generated that is unique to the data to be encrypted since a

particular pattern cannot be reproduced (see column 9, lines (20-30). In addition to generating

true random binary numbers with high statistical quality, generating the values from at least two

oscillators can prevent biased outputs since this technique provides the ability to vary

frequencies and combining the frequencies to avoid biased outputs.

As per claim 12, **Erickson** discloses a field programmable gate array (FPGA): a plurality

of configurable logic elements within the FPGA being programmable with configuration data to

implement a desired circuit design, for example (see column 3, lines 5-21); and a decryption

circuit coupled to received encrypted configuration data, the decryption circuit configured to

decrypt the encrypted configuration data in the FPGA using the fingerprint as a decryption key to

extract the configuration data, for example (see column 3, lines 34-42). **Erickson** discloses a

security circuit comprising a key generator for generating a key (column 2, lines 30-31) and the

security circuit also comprises a security initialization circuit for generating initialization data to

be used for encryption/decryption (column 4, lines 44-65) that meets the recitation of fingerprint

element for generating fingerprint representing inherent manufacturing process variations unique

to the FPGA. **Erickson** does not explicitly disclose generating the key from a ratio of the

number of oscillator counts. **Mos et al** in an analogous art teaches a fingerprint element for

generating fingerprint representing inherent manufacturing process variations unique to the

FPGA (see column 7, lines 1-9 and column 10, lines 44-48), wherein the fingerprint element

includes first and second oscillators and a sensing circuit including, means for counting a first

number of oscillations of a first oscillator and a second number of oscillations of a second

oscillator during a predetermined time interval and means for generating a fingerprint as a ratio

between the first and the second binary numbers of oscillations (see column 14, lines 27-41 and

50-55). **Mos et al** discloses a sensing circuit that meets the recitation of means for truncating m

least significant bits from a first binary number that represents the first number of oscillations

and m least significant bits from a second binary number that represents the second number of

oscillations wherein m is greater than 0 (as shown in figures 4-5 and column 9, lines 37-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention

was made to modify the method of key generation of **Erickson** to apply the concept of random

number generator of **Mos et al** of providing a sensing circuit including means for counting

number of oscillations and generating a ratio as a fingerprint because this circuit provides a way

of generating true random binary numbers with high statistical quality (see column 6, line 63

through column 7, line 9). The motivation to do so is given by **Mos et al** who teaches, a secure

signature is generated that is unique to the data to be encrypted since a particular pattern cannot

be reproduced (see column 9, lines (20-30). In addition to generating true random binary

numbers with high statistical quality, generating the values from at least two oscillators can

prevent biased outputs since this technique provides the ability to vary frequencies and

combining the frequencies to avoid biased outputs.

As per claims 7 and 21, the combination of **Erikson** and **Mos et al** discloses the claimed

method and FPGA of claims 1 and 12 and further discloses wherein the first and second

oscillators comprise configurable logic blocs of the FPGA (see **Mos et al**, abstract).

As per claims 2 and 13, the combination of **Erikson** and **Mos et al** discloses the

limitation configuring the FPGA using configuration data, for example (see **Erikson**, column 3,

lines 39-42).

As per claims 3 and 15, the combination of **Erikson** and **Mos et al** discloses the

limitation of further comprising: transmitting the fingerprint from the FPGA to an encryption

circuit, for example (see column 3, lines 31-32); encrypting the configuration data using the

fingerprint as an encryption key, for example (see column 3, lines 30-35); and storing the

encrypted configuration data in the storage device, for example (see **Erikson**, column 3, lines

15-18).

As per claim 4, the combination of **Erikson** and **Mos et al** discloses the limitation of,

wherein the fingerprint generated during power-up of the FPGA, for example (see **Erikson**,

column 3, lines 25-30).

Conclusion

5.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The

examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carl Colin
Patent Examiner
August 3, 2006

NASSER MOAZZAMI
PRIMARY EXAMINER